UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/052,054	01/17/2002	Timothy W. Kiszely	05655P006	1460

8791 7590 08/11/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
CERVETTI, DAVID GARCIA	
ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 08/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

L

Office Action Summary	**Application No.** 10/052,054	**Applicant(s)** KISZELY, TIMOTHY W.	
	Examiner David G. Cervetti	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 January 2002*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 March 2002* is/are: a)□ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *3/29/02*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-24 are pending and have been examined.

Drawings

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 100, 110 (figure 1), 312, 314, 318 (figure 3). Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "303" has been used to designate both "RAM" (page 14), "operating system" (page 15, line 1), and "co-processor" (page 15, paragraph [45], line 2), perhaps "operating system 318" was intended on page 15, line 1. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should

include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

4. Claim 12 is objected to because of the following informalities: "the method of claim 12 further comprising", perhaps "claim 11" was meant. Examiner has treated claim 12 as stating "the method of claim 11" for the purposes of this document. Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 21 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 21 recites the limitation "the improvement comprising" in line 3 of the claim. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes et al. (NPL Handbook of Applied Cryptography), and further in view of Lim (US Patent Application Publication: 2002/0018562).

Regarding claim 1, Menezes et al. teach a left expansion module and a right expansion module, said left expansion module coupled to a first merged L component key XOR gate and to a third merged L component key XOR gate; said right expansion module (page 253) coupled to a key XOR gate, and to a second merged L component key XOR gate; said key XOR gate coupled to a first selection function module (SFM), the first SFM having a first output and a second output; said first output of the first SFM coupled to a first permutation function module (PFM) and the second output of the first SFM output is coupled to a first merged permutation and expansion function (MPE) module; said first PFM coupled to a second collected L component XOR gate; said first MPE module coupled to the first merged L component key XOR gate, and to the third merged L component key XOR gate; said first merged L component key XOR gate coupled to a second SFM having a first output and a second output; said first output of the second SFM coupled to a second PFM; and said second PFM coupled to a first collected L component XOR gate (pages 250-257). Menezes et al. do not expressly disclose the exact same coupling. Lim teaches an 8-cycle Data Encryption Standard implementation and encryption apparatus (figure 3, pages 3-5). One skilled in the art will recognize that the arrangement is one of many possible arrangements of the logic gates and the permutation and expansion modules, for example, a three-input exclusive or (XOR) gate may be used to replace a pair of two-input XOR gates, and different modules may be combined or split (Lim, paragraph 104).

Regarding claim 2, the combination of Menezes et al. with Lim does not disclose expressly said second output of the second SFM coupled to a second MPE module; said second MPE module coupled to the second merged L component key XOR gate; said second merged L component key XOR gate coupled to a third SFM having a first output and a second output; said first output of the third SFM coupled to a third PFM, and said second output of the third SFM coupled to a third MPE module; said third MPE module coupled to said third merged L component key XOR gate; said third merged L component key XOR gate coupled to a fourth SFM; said fourth SFM coupled to a fourth PFM; and said fourth PFM coupled to the first collected L component XOR gate. However, one skilled in the art will recognize that the arrangement is one of many possible arrangements of the logic gates and the permutation and expansion modules, for example, a three-input exclusive or (XOR) gate may be used to replace a pair of two-input XOR gates, and different modules may be combined (Lim, paragraph 104).

Regarding claim 3, the combination of Menezes et al. and Lim does not expressly disclose wherein the output of the second collected L component XOR gate is coupled to the input of the left expansion module and the output of the first collected L component XOR gate is coupled to the input of the right module function. However, Lim teaches rearranging the functional elements to implement DES in fewer rounds (paragraphs 58-70). Therefore, one skilled in the art will recognize that the arrangement is one of many possible arrangements of the logic gates and the permutation and expansion modules, for example, a three-input exclusive or (XOR) gate may be used to replace a pair of two-input XOR gates, and different modules may be combined.

Regarding claim 4, the combination of Menezes et al. and Lim does not expressly disclose wherein the key XOR gate exclusive-ors the output of the right expansion module and a first sub key block. However, Lim teaches rearranging the functional elements to implement DES in fewer rounds (paragraphs 58-70). The reason for combining is the same as that for claim 3.

Regarding claim 5, the combination of Menezes et al. and Lim does not expressly disclose wherein the first merged L component key XOR gate exclusive-ors the output of the first MPE module, the output from the left expansion module, and a second sub key block. However, Lim teaches rearranging the functional elements to implement DES in fewer rounds (paragraphs 58-70). The reason for combining is the same as that for claim 3.

Regarding claim 6, the combination of Menezes et al. and Lim does not expressly disclose wherein the second merged L component key XOR gate exclusive-ors the output of the second MPE module, the right expansion module, and a third sub key block. However, Lim teaches rearranging the functional elements to implement DES in fewer rounds (paragraphs 58-70). The reason for combining is the same as that for claim 3.

Regarding claim 7, the combination of Menezes et al. and Lim does not expressly disclose wherein the third merged L component key XOR gate exclusive-ors the output from the third MPE module, the left expansion module and a fourth sub key block. However, Lim teaches rearranging the functional elements to implement DES in fewer rounds (paragraphs 58-70). The reason for combining is the same as that for claim 3.

Regarding claim 8, Menezes et al. teach splitting the block of data into a left data block and a right data block; expanding the left data block and the right data block; exclusive-oring, using a key XOR gate, the right expanded data block and a first sub key (page 253); sending the output from the key XOR gate to a first selection function module (SFM), the first SFM having a first output and a second output; sending data at the first output of the first SFM to a first permutation function module (PFM); sending data at the second output of the first SFM to a first merged permutation and expansion function module (MPE); exclusive-oring, using a first merged L component key XOR gate, the output from the first MPE, a second sub key and the expanded left data block; sending the output from the first merged L component key XOR gate to a second SFM, the second SFM having a first output and a second output; sending data at the first output of the second SFM to a second PFM; sending data at the second output of the second SFM to a second MPE; exclusive-oring, using a second merged L component key XOR gate, the output from the second MPE , a third sub key, and the expanded right data block; sending the output from the second merged L component key XOR gate to a third SFM, the third SFM having a first output and a second output; sending data from the first output of the third SFM to a third PFM; sending data at the second output of the third SFM to a third MPE; exclusive-oring, using a third merged L component key XOR gate, the output from the third MPE, a fourth key block, the left expanded data block, and the first MPE; sending the output from the second merged L component key XOR gate to a fourth SFM; and sending the output from the fourth SFM to a fourth PFM (pages 250-257). Menezes et al. do not expressly disclose the exact same coupling. Lim teaches an 8-cycle Data Encryption Standard implementation and encryption apparatus (pages 3-5). One skilled in the art will recognize that the arrangement is one of many possible arrangements of the logic gates and the permutation and expansion modules, for example, a three-input exclusive or (XOR) gate may be used to replace a pair of two-input XOR gates, and different modules may be combined.

Regarding claim 9, the combination of Menezes et al. with Lim does not expressly disclose exclusive-oring the left data block, the first PFM output, and the third PFM output to form a left encrypted data block; and exclusive-oring the right data block, the second PFM output, and the fourth PFM output to form a right encrypted data block. However, Examiner takes Official Notice that the use of three-input XOR gates was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide three inputs to a 3-

input XOR gate since Examiner takes Official Notice that it was conventional and well known (Lim, paragraph 104).

Regarding claim 10, the combination of Menezes et al. with Lim teaches the limitations as set forth under claim 9 above. Furthermore, Lim teaches wherein the left encrypted data block is obtained concurrently with sending the data to the third MPE (pages 3-5).

Regarding claim 11, Menezes et al. teach exclusive-oring, using an exclusive-or gate output from a merged permutation and expansion function module (M.PE), and a sub key block; and sending the output from the exclusive-or gate to a selection function module (pages 250-257). Menezes et al. do not expressly disclose the exact same order of steps or that the permutation and expansion are merged. Lim teaches an 8-cycle Data Encryption Standard implementation (pages 3-5). Therefore, it would have been obvious for such modifications because the same desired effect is acquired. Namely, improve the speed of computing DES. One skilled in the art will recognize that the arrangement is one of many possible arrangements of the logic gates and the permutation and expansion modules, for example, a three-input exclusive or (XOR) gate may be used to replace a pair of two-input XOR gates, and different modules may be combined (Lim, paragraph 104).

Regarding claim 12, the combination of Menezes et al. with Lim teaches the limitations as set forth under claim 11 above. Furthermore, Menezes et al. teach sending output from the selection function module to a permutation function module (pages 250-257).

Regarding claim 13, the combination of Menezes et al. with Lim teaches the limitations as set forth under claim 12 above. Furthermore, Menezes et al. teach sending output from the selection function module to a second MPE (pages 250-257).

Regarding claim 14, Menezes et al. teach a left expansion module and a right expansion module, said left expansion module coupled to a first merged L component key XOR gate and a third merged L component key XOR gate; said right expansion module (page 253) coupled to a key XOR gate, and a second merged L component key XOR gate; said key XOR gate coupled to a first selection function module (SFM), the first SFM having a first output and a second output; said first output of the first SFM coupled to a first permutation function module (PFM) and the second output of the first SFM output is coupled to a first merged permutation and expansion function (MPE) module; said first PFM coupled to a second collected L component XOR gate; said first MPE module coupled to the first merged L component key XOR gate, and to the third merged L component key XOR gate; said first merged L component key XOR gate coupled to a second SFM having a first output and a second output; said first output of the second SFM coupled to a second PFM; and said second PFM coupled to a first collected L component XOR gate (pages 250-257). Menezes et al. do not expressly disclose the exact same coupling or a bus. Lim teaches an 8-cycle Data Encryption Standard implementation and encryption apparatus (pages 3-5). It would have been obvious for the apparatus of Lim to include a bus and processor since it was designed to use registers because the same desired effect was acquired. One skilled in the art will recognize that the arrangement is one of many possible arrangements of the logic gates and the permutation and expansion modules, for example, a three-input exclusive or (XOR) gate may be used to replace a pair of two-input XOR gates, and different modules may be combined.

Regarding claim 15, the combination of Menezes et al. with Lim does not disclose expressly said second output of the second SFM coupled to a second MPE module; said second MPE module coupled to the second merged L component key XOR gate; said second merged L component key XOR gate coupled to a third SFM having a first output and a second output; said first output of the third SFM coupled to a third PFM, and said second output of the third SFM coupled to a third MPE module; said third MPE module coupled to said third merged L component key XOR gate; said third merged L component key XOR gate coupled to a fourth SFM; said fourth SFM coupled to a fourth PFM; and said fourth PFM coupled to the first collected L component XOR gate. However, one skilled in the art will recognize that the arrangement is one of many possible arrangements of the logic gates and the permutation and expansion modules, for example, a three-input exclusive or (XOR) gate may be used to replace a pair of two-input XOR gates, and different modules may be combined (Lim, paragraph 104).

Regarding claim 16, the combination of Menezes et al. and Lim does not expressly disclose wherein the output of the second collected L component XOR gate is coupled to the input of the left expansion module and the output of the first collected L component XOR gate is coupled to the input of the right expansion module. However, Lim teaches rearranging the functional elements to implement DES in fewer rounds (paragraphs 58-70). Therefore, one skilled in the art will recognize that the arrangement is one of many possible arrangements of the logic gates and the permutation and expansion modules, for example, a three-input exclusive or (XOR) gate may be used to replace a pair of two-input XOR gates, and different modules may be combined.

Regarding claim 17, the combination of Menezes et al. and Lim does not expressly disclose wherein the key XOR gate exclusive-ors the output of the right expansion module and a first sub key block. However, Lim teaches rearranging the functional elements to implement DES in fewer rounds (paragraphs 58-70). The reason for combining is the same as that for claim 16.

Regarding claim 18, the combination of Menezes et al. and Lim does not expressly disclose wherein the first merged L component key XOR gate exclusive-ors the output of the first MPE module, the output from the left expansion module, and a second sub key block. However, Lim teaches rearranging the functional elements to implement DES in fewer rounds (paragraphs 58-70). The reason for combining is the same as that for claim 16.

Regarding claim 19, the combination of Menezes et al. and Lim does not expressly disclose wherein the second merged L component key XOR gate exclusive-ors the output of the second MPE module, the right expansion module, and a third sub key block. However, Lim teaches rearranging the functional elements to implement DES in fewer rounds (paragraphs 58-70). The reason for combining is the same as that for claim 16.

Regarding claim 20, the combination of Menezes et al. and Lim does not expressly disclose wherein the third merged L component key XOR gate exclusive-ors the output from the third MPE module, the left expansion module and a fourth sub key block. However, Lim teaches rearranging the functional elements to implement DES in fewer rounds (paragraphs 58-70). The reason for combining is the same as that for claim 16.

Regarding claim 21, Menezes et al. teach an apparatus to perform a DES iteration, said apparatus including an expansion module to receive a R input (page 253), a key XOR, a selection module, a permutation module, and a L component XOR gate, the improvement comprising: a DES circuit to perform a series of iterations that contains no L component XOR gates, said DES circuit to include an expansion module coupled to receive an L input; a merged permutation expansion module, coupled to the selection module of each iteration, that results from merging the permutation module of each iteration with the expansion module of the immediately following iteration in the series; a plurality of merged L component key XOR gates each coupled between a different one of the merged permutation expansion modules and the selection module of the immediately following iteration in the series; a plurality of permutation modules each coupled to one selection module of a different iteration; and a first and second collected L component XOR gates, coupled to mutually exclusive sets of the permutation modules (pages 250-257). Menezes et al. do not expressly disclose the exact same coupling of elements. Lim teaches an 8-cycle Data Encryption Standard implementation (pages 3-5). Therefore, it would have been obvious for such modifications because the same desired effect is acquired. Namely, improve the speed of computing DES. One skilled in the art will recognize that the arrangement is one of many possible arrangements of the logic gates, for example, a three-input exclusive or (XOR) gate may be used to replace a pair of two-input XOR gates.

Regarding claim 22, the combination of Menezes et al. with Lim does not disclose expressly the outputs from the first and second collected L component XOR gates fed back to the expansion module coupled to the L input and the expansion module coupled to the R input respectively. However, Menezes et al. teach using output feedback (pages 228-232). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to feed the output of a gate to the expansion module. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use output feedback as a mode of operation (Menezes et al., pages 228-232).

Regarding claim 23, Menezes et al. teach: a DES circuit having an L and R component input and including, a critical path including, a first and second expansion modules respectively coupled to receive the L and R components (page 253); a plurality of selection function modules coupled to each other in series by a merged permutation and expansion module coupled to a merged L component key XOR gate; a key XOR gate coupled to the first of the selection modules in the series; a first of a plurality of permutation modules coupled to the last of the plurality of selection function modules in the series; and a non-critical path including, a second L component collection XOR module, said first and second L component collection modules coupled to mutually exclusive groups of the plurality of permutation modules, wherein each of the plurality of permutation modules is coupled to a different one of the selection function modules (pages 250-257). Menezes et al. do not expressly disclose the exact same coupling of elements. Lim teaches an 8-cycle Data Encryption Standard implementation (pages 3-5). Therefore, it would have been obvious for such modifications because the same desired effect is acquired. Namely, improve the speed of computing DES. One skilled in the art will recognize that the arrangement is one of many possible arrangements of the logic gates, for example, a three-input exclusive or (XOR) gate may be used to replace a pair of two-input XOR gates.

Regarding claim 24, the combination of Menezes et al. with Lim does not disclose expressly wherein the output from the first L component collection module is fed back to the L component input, and the output from the second L component collection module is fed back to the R component input. However, Menezes et al. teach using output feedback (pages 228-232). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to feed the output of a gate to the expansion module. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use output feedback as a mode of operation (Menezes et al., pages 228-232).

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100